

**SWE-P30-02**

**新版telnet说明文档**

**V1.00**

**修 订 记 录**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 编号 | 修订内容简述 | 修订人 | 修订日期 | 修订后版本号 |
| 1 | 创建文档 | 邵培杰 | 2013-10-12 | V1.00 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**目录**

[**1.** **简介** 4](#_Toc370749145)

[**1.1.** **目的** 4](#_Toc370749146)

[**1.2.** **新版telet引入时间** 4](#_Toc370749147)

[**2.** **新版telnet操作手册** 5](#_Toc370749148)

[**2.1.** **登陆telnet** 5](#_Toc370749149)

[**2.2.** **锁定telnet服务** 5](#_Toc370749150)

[**2.3.** **强制解除telnet锁定** 6](#_Toc370749151)

[**3.** **新版telnet实现** 6](#_Toc370749152)

[**3.1.** **原版telnetd原理** 6](#_Toc370749153)

[**3.2.** **原版login原理** 8](#_Toc370749154)

[**3.3.** **telnet登陆模型** 10](#_Toc370749155)

[**3.4.** **新版telnet原理** 10](#_Toc370749156)

[**4.** **调试** 13](#_Toc370749157)

关键词：*telnet telnetd login busybox*

摘要：介绍新版telnet登陆操作方法和新版telnet原理、

缩略语清单：*对本文所用缩略语进行说明，要求提供每个缩略语的英文全名和中文解释。*

| 缩略语 | 英文全名 | 中文解释 |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. **简介**

Telnet最初是由ARPANET开发，现在主要用于Internet会话。它的基本功能是，允许用户登录进入远程主机。它让用户的本地计算机与远程计算机连接，从而成为远程主机的一个终端。新版telnet在本公司原有telnet用户名和密码无法更改的基础上，将telnet账户和密码绑定到设备系统本地和WEB端密码，从而实现用户名密码可变，增加telnet系统安全性。

* 1. **目的**

本公司大多数设备使用的根文件系统为Cramfs只读文件系统，而telnet登陆依赖linux系统账户和码配置文件/etc/passwd，这样就造成telnet用户名和密码无法变更的问题，因此长期以来，telnet都使用固定用户和密码登陆，典型值为用户名：root 密码： vizxv。

这样做的后果是telnet密码容易泄露或被暴力破解出来，设备很可能遭受到网络攻击或者非法用户登陆并恶意操作导致系统瘫痪等。因此在经过多次会议讨论后最终设计方案如下：

（1）telnet登陆用户名为应用admin组用户任意用户

（2）为了体现telnet只开放给开发人员的特性，密码为7ujMko0+该用户密码

（3）telnet用户或密码如果三次输入失败，则锁定telnet服务30分钟。

* 1. **新版telet引入时间**

SVN： http://10.6.5.2/svn/DVR\_Tools/Busybox/Busybox\_N5/Trunk

版本： 2342

1. **新版telnet操作手册**

本节描述telnet登陆操作，以及锁定后的解锁方法等。

* 1. **登陆telnet**

（1）**正常登陆**

正常登陆情况是指应用没有清除配置文件，或者应用清除配置文件后已经生成默

认配置文件的情况，本质表现为存在/mnt/mtd/Config/passwd或者/mnt/mtd/Config/Account1密码文件。

**用户名：** 应用admin组任意一个用户，如admin、888888等；

**密码：** 7ujMko0+该用户密码（不带+）；

补充说明： 7ujMk(小写字母o)（数字0）；

特别的： 如果该用户密码为空，则仅需输入7ujmKo0即可；

（2）**异常登陆**

如果不存在/mnt/mtd/Config/passwd或者/mnt/mtd/Config/Account1密码文件——可能的原因是开发过程中手动删除了配置文件，而此时又没有启动应用(appauto=0)自动创建默认配置文件。

**用户名：** root

**密码：** 7ujMko0vizxv

* 1. **锁定telnet服务**

当尝试登陆telnet用户名或者密码错误累计超过3次时，30分钟内telnet服务将拒绝新的telnet登陆，但对那些之前已经登陆的用户则没有影响。 累计的策略是：

（1）全局累计制，如当前有两个用户尝试登陆，则两个用户的出错次数相加；

（2）如果有一个用户登陆成功，则全局错误累计数清零，此时出错用户再次获得3次机会；

（3）系统重启后全局错误累计数清零；

* 1. **强制解除telnet锁定**

在开发/调试过程中，如果不慎锁住了telnet服务，则可以选以下**任意一种**方法解除telnet锁定：

（1）如果允许，删除本地文件/var/.login\_lock（隐藏文件）；

（2）如果允许，重启系统；

（3）如果允许，将系统时间播快30分钟或以上；

1. **新版telnet实现**

本文档介绍的telnet原理基于busybox-1.18.4，与tenlet服务的相关程序有：

1. telnetd： telnet服务端程序
2. login： 负责登陆系统时接受/校验用户名和密码，并最终执行shell程序
3. sh： shell程序，命令行交互程序
   1. **原版telnetd原理**

Telnetd是telnet服务端程序，他主要的工作有两点，一点是维持TCP服务，接受和处理来自远程的连接请求和数据传输；另一点是创建交互式程序login程序，并通过pty将数据转发到客户端或者从客户端转发数据到pty从设备端。实际上telnetd只是充当数据传输的桥梁，仅此而已。telnetd程序的流程图如下图3-1所示：



图3-1 telnetd软件流程图

其中：

G.session是telnetd的一个全局链表，用于保存每个连接到telnet的会话的指针；

buff1和buff2是为每个会话创建的两个缓冲区，他们的工作机制可以在telnetd的代码注释中得到，如图3-2所示：

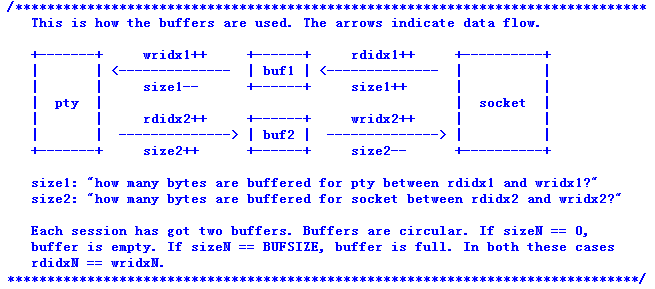


图3-2 telnetd缓冲机制

从中我们可以看出，telnetd服务为单线程方式，通过select管理并发操作，这样，我们就能够在图3-1中红色部分（accept操作）对telnet客户端的连接进行控制。

* 1. **原版login原理**

login程序主要处理用户登陆系统，包括用户名校验，权限校验，密码校验等。假如这些检查都通过，则login程序会调用exec运行shell程序。因为login具有setuid属性，因此login实际上以root权限运行，在运行shell之前需要将系统权限降到该用户的有效用户权限。当我们登陆一个linux系统时，通常第一个与我们交互的程序是login，其次是shell。Login的执行流程如图3-3所示：



图3-3login流程

* 1. **telnet登陆模型**

当我们尝试通过telnet登陆系统时，客户端和服务端呈现的模型如图3-4所示：



图3-4 telnet通信模型

客户端通过TCP/IP连接到telnetd的23号端口(通常是23)，而telnetd的处理是创建一个login进程，将login的标准输入输出都替换为pty从设备。Telnetd同时监听pty主设备和socket事件：当socket有数据时，读socket并将数据写入pty从设备；当pty从设备可读时，读取数据发送到socket客户端。从telnet客户端和login向外看，telnetd是透明的，也即他们根本不知道telnetd的存在。

* 1. **新版telnet原理**

新版telnet在busybox1.18.4自带telnet和login代码上进行了修改。注意图3-1和图3-3中红色部分，这些部分是实现新版telnet锁修改的模块。我们通过修改telnetd的代码，使它能够在检测到一个新的socket连接判断该链接是否合法，是否拒绝服务；我们通过修改login代码，使得不管输入什么用户名，login都用root用户登陆(这样设计是因为系统无法修改/etc/passwd以便添加新的用户)；而在密码校验阶段，我们在login中插入大华的加密算法，然后校验输入的用户名和密码，并将密码校验的结果作为root密码的校验结果，这样一来，我们就能以root的名义，而非root真实密码登陆系统。

**3.4.1** 新版telnetd与login通信模型

为了实现3次输入失败锁定30分钟功能，我们建立一个文件/var/.lockin\_lock 来联系telnetd和login进程：

1. 当该文件不存在时，说明系统没有登录失败记录，可以正常登陆；
2. 当文件存在同时内部计数器小于3时，可以正常登陆；
3. 当文件存在且计数器大于等于3时，则锁定telnet登陆，且每次有telnet登陆

时都会与文件中记录的时间戳比较，直到30分钟期限到；

（4）当有用户成功登陆时，删除该文件，telnet恢复到（1）状态；

telnetd与login的联系如图3-5所示：



图3-5 telnetd与login的联系

**3.4.2** 新版login代码流程

新版login的代码流程如图3-6所示(仅部分)：



图3-6 新版login代码流程

其中：

correct\_password\_ext函数用于校验大华应用的用户名和密码，函数直接解析应用生成的password文件。目前，应用有两套加密机制，密码文件分别为/mnt/mtd/Config/passwd

和/mnt/mtd/Config/Account1。passwd多数被存储产品DVR/NVR等使用，Account1大多被前端所使用，且安全性更好，未来DVR/NVR可能会切换到该加密方式。

**3.4.3** 新版telnetd代码流程

新版telnetd的代码流程如图3-6所示(仅部分)：



图3-6 新版telnetd的代码流程

新版telnetd程序对文件中记录的错误次数进行判断，次数大于等于3则直接拒绝登陆，并提示锁定信息。此外，telnetd程序还会判断文件中的的时间戳与当前时间戳，当30分钟超时时间已经达到时，telnetd会删除文件，恢复服务。

1. **调试**

调试telnet有多种方法，最直接的方法是重新打包烧写，并测试。这种方式的缺点很明显，非常不利与调试，适合于发包测试。这里介绍一种调试方法，可用于调试telnet登陆。本人将该方法命名为：替换/bin法。

以本人的编译服务器为例，步骤如下：

（1）在设备上： ~# kill 当前telnetd进程PID

（2）在设备上： ~# mount -t nfs -o nolock,tcp 10.6.5.53:/share/shaopeijie/ /nfs

（3）在设备上： ~# cp -a /bin /nfs/copy\_bin 报错忽略之

（4）在服务器上： 替换/share/shao\_peijie/copy\_bin/下的busybox

（5）在设备上： ~# mount -t nfs -o nolock,tcp 10.6.5.53:/share/shaopeijie/copy\_bin /bin

（6）在设备上： ~# telnetd

（7）测试telnet功能，如有问题，则重复（1） （4） （6）即可